However, biometric parameter analysis can be considerably more complicated than processing password or token data as it requires specialized hardware.

[0013] A further complicating factor in the field of secure transactions is that trends in microprocessor-based hardware are moving away from the traditional desk-bound personal computers. Hybrid devices such as mobile phones, PDAs and tablet-based computers are themselves now practical for use as authentication devices.

[0014] One of the major applications for secure user authentication is in the field of e-commerce. Here e-commerce is understood to include mobile financial transactions such as credit card payment, online ordering and similar. In this context it is desired that a user be able to provide transaction authentication information from mobile locations quickly, easily and securely.

[0015] To this end, and coupled with improvements in wired and wireless bandwidth capability, it is possible to access highly sensitive data using such devices. For example a handheld PDA running a thin-client browser coupled with a mobile phone can be used to access an internet banking website in order to carry out highly trust-sensitive financial transactions. At present, such transaction contexts are protected using the secure socket layer (SSL) protocol under HTTP. However, this technique is relatively inflexible and essentially corresponds to a binary authentication method where the transaction context is assumed to be static once the user is initially authenticated.

[0016] Of course there is a broad spectrum of what constitutes a trust-sensitive transaction. Devices such as cellphones can now be used as simple payment mechanisms in the context of billing vending machine transactions to a users mobile telecoms account and similar small-value transactions.

[0017] Notwithstanding this, user authentication is critical to the acceptance and practicality of secure transactions. Thus, there is an ongoing need for systems which provide reliable authentication and which are extensible in the context of future developments in user devices, paradigms and the networks over which such devices communicate.

[0018] The present invention attempts to overcome or at least ameliorate a number of the abovementioned limitations inherent in the present techniques as well as anticipating some issues raised by evolving usage habits emerging from take-up of new technology.

DISCLOSURE OF THE INVENTION

[0019] In one aspect the invention provides for a method of authenticating a users ability to carry out a transaction, the method including the steps of:

[0020] a user initiating an authentication request in order to carry out a secure transaction;

[0021] dynamically collecting and assessing a plurality of confidence parameters, said confidence parameters reflecting factors related to the security of the transaction context; and

[0022] dynamically maintaining a confidence level based on the plurality of confidence parameters whereby if the confidence level drops below a predetermined confidence threshold, the transaction is not authenticated and if the confidence level exceeds a predetermined confidence threshold, the transaction is authenticated.

[0023] The predetermined confidence threshold preferably reflects the sensitivity of the transaction.

[0024] In an alternative embodiment, a static confidence window may be defined in response to substantially static confidence parameters, the confidence window having an upper and lower limit reflecting an inherent upper and lower limit that the confidence level can reach.

[0025] Preferably in the method as hereinbefore defined, user authentication is inhibited if the confidence threshold of the transaction is outside the confidence window.

[0026] The user preferably alters the confidence level, either autonomously or in response to an external request, by varying and/or adding one or more confidence parameters.

[0027] The confidence level may vary with time and/or transaction context.

[0028] Alternatively, the confidence level may decay over time.

[0029] The confidence parameters may include:

[0030] intrinsic context parameters such as user input device security, user location, user identity, multiple user co-location, time after users authentication request initiation, required transaction security level, required resource security level and the like; and/or

[0031] extrinsic context parameters such as changes in network characteristics, dynamic changes in the sensitivity of the transaction and the like.

[0032] In a preferred embodiment, the transaction corresponds to a user requesting access to a resource.

[0033] The confidence threshold may change as a function of the capability of the users input device.

[0034] In an alternative embodiment, the confidence level is preferably determined based the confidence parameters and /or on accumulated statistical data relating to the behaviour of the user.

[0035] In a further aspect, the invention provides for a system for dynamically authenticating a transaction, the system including:

[0036] a confidence engine adapted to:

[0037] dynamically maintain at least one confidence level by monitoring a plurality of confidence parameters, the confidence level reflecting the security of the transaction context;

[0038] compare the derived confidence level with a predetermined confidence threshold, the confidence threshold reflecting the security required to perform the transaction;

[0039] when the confidence level is below the confidence threshold, requesting new confidence parameters or varying existing confidence parameters; and